

COMPUTER NETWORK SECURITY SYSTEM

Abstract of the Disclosure

A method and system are provided for authenticating a user of a computer over a computer network. In one embodiment of the invention, the method includes transmitting an applet having a challenge string and a first encryption key, receiving a login packet having the challenge string and a password that is encrypted using the first encryption key, decrypting the password, receiving information from an authentication provider, and authenticating the password by using the information provided by the authentication provider. The challenge string can be either a sequence number or a session identifier. The login packet can further include a user name, wherein the session identification, the user name, and the password are encrypted. Additionally, the login packet can include a hash of the session identification, the user name, and the password. Authenticating the password by using an authentication provider can include receiving from an authentication provider a second encryption key; encrypting using the second encryption key and transmitting to the authentication provider the password, receiving from the authentication provider a second hash of the password and a character string; and determining from the character string if the password is correct. The authentication provider can be a software program or an authentication server. An advantage of embodiments of the present invention is that a computer can provide secure Internet communications using a web browser that does not support SSL and can provide secure integration with third party security systems.